Недашківський Г. В., магістрант, гр. ІПЗм-21-2
Державний університет «Житомирська політехніка»

НЕМОЖЛИВІСТЬ ЗБЕРЕЖЕННЯ КОНФІДЕНЦІЙНОСТІ У СОЦІАЛЬНИХ МЕРЕЖАХ

Занепокоєння користувачів соціальних мереж щодо їхньої конфіденційності різко зросло в останні роки. Випадки витоку даних викликали занепокоєння багатьох користувачів і змусили їх переглянути свої стосунки з соціальними мережами та безпеку їх особистої інформації. Прикладом цього є драматична історія консалтингового агентства Cambridge Analytica. Фірма використовувала особисту інформацію понад 50 мільйонів користувачів Facebook, щоб вплинути на президентські вибори в США 2016 року. Цей та інші приклади неухильно погіршили довіру громадськості та призвели до того, що багато користувачів замислюються, чи не втратили вони контроль над власними даними. Згідно з дослідженням, проведеним Pew Trust, 80 відсотків користувачів соціальних мереж повідомляють, що їх турбує бізнес і рекламодавці, які отримують доступ до їхніх публікацій у соціальних мережах і використовують їх. Ці зростаючі занепокоєння конфіденційністю спонукали до пропаганди жорсткіших правил. Крім того, вони посилили контроль над компаніями, відповідальними за захист персональних даних.

Враховуючи сучасні проблеми та занепокоєння щодо конфіденційності соціальних мереж, кваліфіковані фахівці з кібербезпеки відіграватимуть життєво важливу роль у захисті даних і особистої інформації користувачів соціальних мереж.

Що хвилює користувачів соцмереж? Чи виправдані їхні хвилювання? Як правило, ці занепокоєння виникають через всюдисущу присутність соціальних мереж у житті людей. Сорок п'ять відсотків населення світу користується соціальними мережами. Відповідно до даних, зібраних Hootesuite, це означає, що приголомшливі 3,48 мільярда людей підключаються до тих чи інших соціальних мереж. Ці з’єднання можуть зробити користувачів уразливими кількома способами. Коли особиста інформація потрапляє в чужі руки, наслідки можуть бути згубними. За даними Pew Trust, облікові записи 13 відсотків американців заволоділи неавторизованими користувачами. Такі зломи можуть призвести до викраденої інформації та примусового поширення, що перенаправляє підписників на зловмисне програмне забезпечення, серед іншого. Загалом, платформи соціальних медіа, які збирають і зберігають величезні обсяги особистої інформації з обмеженим державним контролем, є привабливими цілями для зловмисників, які прагнуть використовувати ці дані для шахрайства та крадіжки.

Ще одне зростаюче занепокоєння, посилене порушенням даних Facebook компанією Cambridge Analytica, зосереджується на тому, як зловмисники отримують доступ до приватних даних із платформ соціальних мереж та інших місць і використовують їх для маніпулювання думкою на користь кількох людей. Наприклад, російську операцію «Агентство інтернет-досліджень» звинувачують у втручанні у президентські вибори в США 2016 року через використання соціальних мереж для поширення дезінформації, яка розпалила конфлікт і недовіру.

Злочинці вправно намагаються змусити користувачів соціальних мереж надати конфіденційну інформацію, викрасти особисті дані та отримати доступ до облікових записів, які користувачі вважають конфіденційними. Нижче наведено типові загрози в соціальних мережах.

1. Видобуток даних – (Кожен залишає за собою дані в Інтернеті.)
2. Спроби фішингу – (Фішинг — один із найпоширеніших способів, якими злочинці намагаються отримати доступ до конфіденційної особистої інформації.)
3. Обмін шкідливими програмами – (Зловмисне програмне забезпечення призначене для отримання доступу до комп’ютерів і даних, які вони містять.)
4. Ботнет-атаки – (Боти соціальних мереж — це автоматизовані облікові записи, які створюють дописи або автоматично підписуються на нових людей щоразу, коли згадується певний термін.)

Атаки, описані вище, продовжуватимуть становити загрозу конфіденційності. Фактично, з наближенням президентських виборів, кількість таких атак, ймовірно, збільшиться. Раніше цього року Politico повідомляло, що широкомасштабні кампанії дезінформації, спрямовані проти кандидатів, вже почалися. Зловмисники, тепер використовують дані соціальних мереж, щоб вести дезінформаційну «війну», покликану ввести в оману та поляризувати суспільство. Кіберпропаганда часто поширюється через облікові записи ботів, які використовують видобуті дані для націлювання на бажану аудиторію. Видалення вашого облікового запису може допомогти обмежити обсяг доступної в інтернеті інформації про вас, це не є надійним способом гарантувати, що ваші дані не будуть скомпрометовані.

Хоча існує багато причин, чому соціальні медіа шкодять вашій безпеці та конфіденційності, вони надають можливість для звичайних і професійних користувачів дізнатися, як краще захистити вашу інформацію в Інтернеті.